

Remarks

Claims 23-29 have been cancelled. Claim 30, indicated as being allowable if rewritten in independent form, has been rewritten in such form.

Claims 1-3, 5, 8, 10-12, 14-19 and 21 stand rejected under 35 U.S.C. § 103 as being unpatentable over U.S. Patent 6,510,520 to Steinberg in view of U.S. Patent 5,949,877 to Traw et al. ("Traw") (paper no. 9, page 2, ¶ 3), while claims 4 stands rejected under 35 U.S.C. § 103 as being unpatentable over Steinberg in view of Traw and U.S. Patent 5,465,300 to Altschuler et al. ("Altschuler") (paper no. 9, page 4, ¶ 4), and claims 13, 20 and 20-22 stand rejected under 35 U.S.C. § 103 as being unpatentable over Steinberg in view of Traw and Schneier, Applied Cryptography, Second Edition ("Schneier") (paper no. 9, page 4, ¶ 5). These rejections are respectfully traversed.

Each of these claims is dependent on one of three independent claims: 1, 15 and 21. Each of these independent claims is in turn directed to an implementation in which a first device authentication is performed between an input device and an memory device when writing digital data from the input device to the memory device, while a second device authentication is performed between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device.

Steinberg discloses a digital camera system in which a secure storage device 10 (Fig. 1) intermediating between a camera and a user's computer is used to either encrypt a digital image or generate a signature on the image. The ultimate user, not the secure storage device, either decrypts the image or authenticates the digital signature, depending on the type of processing performed by the secure storage device.

Traw discloses a method for protecting digital content from "copying and/or other misuse" as it is transferred between devices over insecure links; the method includes the step of authenticating that both a content source and a content sink are compliant devices (col. 1, lines 42-45).

The Examiner argues that it would have been obvious to performing a first device authentication between the input device and the memory device a second device authentication between the memory device and the receiving device "to prevent copying and/or misuse of the data during transfer", adding that one of ordinary skill would have been motivated to perform such a modification "to prevent copying and/or other misuse of the data" (paper no. 9, page 3).

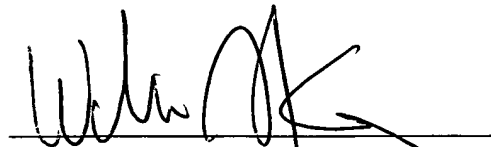
However, applicants are concerned not with "copying or other misuse" of data, but rather with authenticating such data and protecting it against alteration by someone seeking, for example, to perpetrate an insurance fraud (specification, page 1). It is not at all apparent why one concerned with guarding against data alteration would look to a copy protection mechanism for guidance. Accordingly, one cannot properly combine Steinberg with Traw to obtain applicants' invention.

Conclusion

For the foregoing reasons, claims 1-5, 8 and 10-22 as previously presented and claim 30 as currently amended are believed to distinguish patentably over the art cited by the Examiner. Entry of this amendment and reconsideration of the application as amended are respectfully requested. It is hoped that upon such consideration, the Examiner will hold all claims allowable and pass the case to issue at an early date. Such action is earnestly solicited.

Respectfully submitted,
KOICHI KAMIJO et al.

By



William A. Kinnaman, Jr.

Registration No. 27,650

Phone: (845) 433-1175

Fax: (845) 432-9601

WAK/wak